Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”

CENTRUL DE STUDII STRATEGICE DE APĂRARE ȘI SECURITATE

Nr. 2 (161) / 2019
Indexat în CEEOL

COOPERAREA CIVILI-MILITARI ÎN CADRUL OPERAŢIILOR INFORMAŢIONALE

Petre Răzvan ENACHE

Civil military cooperation in information operations

Abstract: *The information operations carried out at all levels (strategic, operational, tactic) can be one of the most appropriate responses that the military institution can give to modern threats. In order to achieve the objectives of information operations, firearms may sometimes be used to hit specific targets. There are also some capabilities, tools and techniques or specialized key elements which are the basis of most information activities. We identify, therefore, in the allies' conception Civil-military cooperation/CIMIC as part of information operations and a specific tool of civil-military interaction.*

Keywords: *information operations, civil-military cooperation, threats, effects.*

Cooperarea civili-militari în cadrul operațiilor informaționale

Rezumat: *Operaţiile informaţionale desfăşurate la toate nivelurile (strategic, operativ, tactic) pot constitui unul din cele mai adecvate răspunsuri pe care instituţia militară îl poate da ameninţărilor moderne. În scopul realizării obiectivelor în domeniul operaţiilor informaţionale, uneori pot fi folosite mijloace de foc pentru lovirea unor ţinte specifice. De asemenea, există câteva capabilităţi, instrumente şi tehnici sau elemente cheie specializate, care constituie baza celor mai multe activităţi informaţionale. Identificăm, în concepţia aliaţilor, cooperarea civili-militari/CIMIC ca fiind parte componentă a operaţiilor informaţionale, dar şi instrument specific al interacţiunii civil-militare.*

Cuvinte-cheie: *operaţii informaţionale, cooperare civili-militari, ameninţări, efecte.*

Introducere

Dezvoltarea intensă a domeniului informaţional pe plan mondial a impus armatelor moderne şi, implicit, Armatei României, formularea unui răspuns la noile provocări survenite ca urmare a extinderii şi perfecţionării mediului informaţional, precum şi adoptarea unor măsuri în consecinţă, ce vizează, deopotrivă, reducerea propriilor vulnerabilităţi şi exploatarea celor care aparţin adversarului.

Operaţiile informaţionale reprezintă o funcţie de stat major şi constituie atât un multiplicator de forţă, cât şi un mecanism integrator

Petre Răzvan ENACHE, *instructor superior în Departamentul Forțe Terestre/Facultatea de Comandă și Stat Major din cadrul Universității Naționale de Apărare „Carol I” București, este doctorand în domeniul Științe Militare în aceeași instituție academică (e-mail: razvann_enache@yahoo.com).*

şi de coordonare, ce contribuie la sprijinirea comandanţilor în atingerea obiectivelor acestora şi, implicit, a forţelor proprii în îndeplinirea misiunilor ce le revin. Operaţiile informaţionale desfăşurate la toate nivelurile (strategic, operativ, tactic) pot constitui unul din cele mai adecvate răspunsuri pe care instituţia militară îl poate da ameninţărilor moderne.

În cadrul funcţiilor de luptă, identificăm *activităţile informaţionale* ca fiind „acele acţiuni ce au drept scop modificarea informaţiei şi/sau a sistemelor informaţionale, care pot fi executate de orice actor şi includ măsuri de protecţie”[1].

Conceptul de *operaţii informaţionale/INFO OPS* a fost utilizat de către armata americană în anul 1995 şi descria importanţa informaţiei şi cum se poate câştiga războiul informaţional în operaţiile militare în secolul XXI. Pentru prima dată, *operaţiile informaţionale* erau definite ca „operaţii militare continue în cadrul mediului informaţional militar care permit, îmbunătăţesc şi protejează ciclul decizional al comandantului, precum şi modul de executare al misiunilor pentru obţinerea avantajului informaţional în întreaga gamă a operaţiilor militare. Info Ops includ şi interacţiunea cu mediul informaţional global şi, după cum este necesar, exploatarea sau afectarea sistemului informaţional şi cel decizional al inamicului”[2].

1. Abordări ale operaţiilor informaţionale

În anul 1995, specialiştii militari americani au început să utilizeze un nou concept, acela de *operaţii informaţionale*, identificând informaţia ca un factor esenţial al puterii militare la nivel strategic, operativ şi tactic şi detaliind modul în care informaţia contribuie la succesul misiunii forţelor aliate şi înfrângerea inamicului, ca parte integrantă a operaţiilor militare. Ulterior, urmare a experienţelor acumulate de militarii americani în desfăşurarea operaţiilor informaţionale, conceptul a fost dezvoltat şi, începând cu anul 2006, acesta se referă la „utilizarea integrată a războiului electronic/EW, a operaţiilor în reţele de calculatoare/CNO, a operaţiilor psihologice/PSYOPS, a inducerii în eroare/MILDEC şi a securităţii operaţiilor/OPSEC, împreună cu capabilităţile de sprijin şi conexe specifice, pentru a influenţa, distruge, corupe sau perturba procesul uman sau automatizat de luare a deciziei de către inamic, simultan cu protejarea propriilor procese”[3].

Spre deosebire de armata americană, conceptul aliat de *INFO OPS* se referă la „acele procese coordonate, în continuă mişcare, care reunesc activităţile diplomatice, politice şi militare ale NATO pentru influenţarea factorilor de decizie non-NATO în sprijinul obiectivelor Alianţei”[4]. Ca şi în cazul doctrinei aliate, britanicii fac totuşi precizarea că este esenţial ca ofiţerii care lucrează în operaţiile ce implică mass-media să coopereze strâns cu cei ce desfăşoară *INFO OPS* pentru a se asigura că mesajul dorit este transmis audienţei avute în vedere. *INFO OPS* britanice deosebesc activităţile de influenţare a voinţei şi pe cele de contracarare a capacităţilor de comandă ale inamicului, fără a le mai evidenţia, precum în doctrina NATO sau doctrina SUA, pe cele de protecţie informaţională. Totuşi, instrumentele operaţionale sunt, în esenţă, aceleaşi ca în cazul armatei SUA sau la nivelul Alianţei, adică operaţiile psihologice, inducerea în eroare, distrugerea fizică, operaţiile în reţelele de calculatoare, războiul electronic, la care se mai adaugă unele tehnologii neconvenţionale care sunt necesare. Cert este că şi britanicii, la fel ca şi americanii şi aliaţii, subliniază faptul că *INFO OPS* reprezintă o strategie integratoare şi nu o capacitate de luptă propriu-zisă şi că prin *INFO OPS* nu se comandă nicio capacitate militară, ci se integrează şi se sincronizează, ca parte a managementului unei campanii, o categorie largă de activităţi destinate să îndeplinească obiectivele comandantului forţei întrunite.

În concepţia Chinei, operaţiile informaţionale sunt operaţii specifice considerate a fi în centrul războiului informaţional, în acelaşi mod în care acesta este considerat a fi în centrul conceptului de informatizare. *INFO OPS* chineze sunt considerate a fi manifestarea răz-

boiului informaţional pe câmpul de luptă. Acestea pot fi atât defensive, cât şi ofensive şi pot fi derulate la nivel strategic, operativ şi tactic[5].

Abordarea războiului informaţional/operaţiilor informaţionale din perspectiva Rusiei diferă într-o oarecare măsură faţă de concepţia ţărilor vestice. Din punctul de vedere al Moscovei, informaţia este în sine o valoare care are nevoie să fie protejată în timp de pace şi de război. După o analiză a doctrinei ruseşti privind războiul informaţional şi operaţiile informaţionale rezultă câteva elemente care le conferă unicitate[6], cum ar fi: perioada de tranziţie a statului, economiei şi societăţii este îndelungată, ceea ce induce o vulnerabilitate a maselor la acţiuni de manipulare; gândirea militară tradiţională rusă, dezvoltată diferit faţă de cea vestică, sub influenţa considerentelor geografice, a varietăţii ameninţărilor şi realităţilor economice şi-a pus amprenta asupra modului de utilizare a informaţiilor ca armă, dar şi asupra infrastructurii şi capacităţilor restrânse specifice tehnologiei informaţiei.

2. Cooperarea civili-militari ca parte integrantă a operaţiilor informaţionale

În scopul realizării obiectivelor în domeniul operaţiilor informaţionale, uneori pot fi folosite mijloace de foc pentru lovirea ţintelor specifice. Totodată, există „câteva capabilităţi, instrumente şi tehnici sau elemente cheie specializate care formează baza celor mai multe activităţi informaţionale. Acestea sunt: operaţiile psihologice; influenţarea prin prezenţă, postură şi profil; securitatea operaţiilor; asigurarea securităţii informaţiilor; inducerea în eroare/mascarea; războiul electronic; distrugerea fizică; angajarea liderilor cheie; operaţiile în reţeaua informatică şi cooperarea civili-militari”[7].

Identificăm, aşadar, în concepţia aliaţilor, *cooperarea civili-militari/CIMIC* ca fiind parte componentă a operaţiilor informaţionale/*INFO OPS*. Rolul *CIMIC* în cadrul acestor tipuri de operaţii este unul important, în special datorită contactului permanent pe care elementele CIMIC îl menţin cu ceea ce generic numim *actori civili*, înţelegând prin aceştia autorităţi naţionale, regionale şi locale, organizaţii civile, dar şi populaţia locală. Astfel, obiectivele operaţiilor informaţionale sunt susţinute prin activităţi CIMIC desfăşurate în zona de responsabilitate.

CIMIC este unul din instrumentele specifice al *interacţiunii civil-militare/CMI*, prin care se realizează coordonarea şi cooperarea între comandantul forţei militare şi actorii civili, cum ar fi populaţia şi autorităţile locale, organizaţiile civile, agenţiile internaţionale şi naţionale, guvernamentale şi neguvernamentale, ce acţionează în sprijinul misiunii.

În vederea realizării scopului *CIMIC* sunt necesare forţe specializate, organizate şi dimensionate în funcţie de natura misiunii. Modul de augmentare/sprijinire al diferitelor structuri cu elemente CIMIC diferă în funcţie de tipul şi obiectivele misiunii. Principial, o companie CIMIC este pusă la dispoziţia unei divizii pentru executarea misiunilor de sprijin în zona de responsabilitate a acesteia, un pluton CIMIC la dispoziţia unei brigăzi şi echipe tactice CIMIC în sprijinul batalioanelor.

Punctul nostru de vedere este că, atunci când se stabileşte dimensiunea şi organizarea elementului CIMIC destinat pentru a sprijini o structură militară, ar trebui analizată situaţia în detaliu, ţinând cont de toate aspectele specifice şi anume: ce tip de operaţie se desfăşoară, ce fază a operaţiei se derulează, particularităţile zonei de responsabilitate, prezenţa organizaţiilor civile, situaţia civilă din zona de responsabilitate etc. Astfel, configuraţia elementului CIMIC destinat unei structuri militare poate diferi în funcţie de misiunea acesteia.

Elementele CIMIC vor desfăşura activităţi specifice pentru evaluarea situaţiei civile din zona de responsabilitate şi a infrastructurii, precum şi pentru estimarea privind evoluţia viitoare a acestei situaţii. Permanent, elementele CIMIC actualizează evaluările zonei de responsabilitate prin interacţiunea frecventă cu comunităţile locale. O legătură permanen-

tă va fi asigurată de către elementele CIMIC cu autorităţile din zona de responsabilitate. De asemenea, pe baza evaluărilor realizate, a discuţiilor cu liderii locali şi cu populaţia civilă, dar ţinând cont de misiunea structurii pe care o sprijină, elementele CIMIC vor identifica, iniţia şi dezvolta proiecte cu impact imediat. Mai mult, elementele CIMIC vor coopera îndeaproape cu organizaţiile civile din zonă în scopul eliminării duplicării eforturilor şi identificării în comun a soluţiilor şi resurselor necesare sprijinirii mediului civil.

Astfel, rolul *cooperării civili-militari* în cadrul *operaţiilor informaţionale* este semnificativ, sprijinind îndeplinirea obiectivelor campaniei informaţionale şi desfăşurând activităţi specifice conform acesteia.

Concluzii

Operaţiile informaţionale/INFO OPS au scopul de a obţine superioritatea în faţa inamicului prin afectarea informaţiilor acestuia, utilizând diferite metode şi tehnici specifice acestui tip de acţiune militară, concomitent cu protecţia propriei resurse informaţionale, evitând astfel orice potenţial atac asupra ei.

Cooperarea civili-militari/CIMIC este o parte componentă a operaţiilor informaţionale şi contribuie semnificativ la îndeplinirea obiectivelor campaniei informaţionale. Elementele CIMIC deţin un rol important în cadrul operaţiilor informaţionale, în special datorită interacţiunii permanente cu actorii civili.

Considerăm oportună creşterea în importanţă a acestor tipuri de acţiuni în special având în vedere că au rolul de multiplicator de forţă şi pot contribui la obţinerea unor efecte semnificative cu resurse mai reduse.

Note bibliografice:

[1] *AJP-3.2 – Allied Joint Doctrine for Land Operations*, March 2016, pp. 2-16.

[2] *TRADOC Pamphlet 525-69 – Concept for Information Operations*, Department of the Army, August 1995, p. 1.

[3] *Joint Publication 3-13 – Information Operations*, February 2006, p. 3.

[4] *AJP-3.10 – Allied Joint Doctrine for Information Operations*, November 2009, pp. 1-6.

[5] Vinod Anand, „Chinese Concepts and Capabilities of Information Warfare”, *Strategic Affairs*, Volume 30, Issue 4, Institute for Defense Studies and Analyses, October 2006, p. 13.

[6] Timothy L. Thomas, *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*, Special Study No. 98-21, Foreign Military Studies Office, September 1998, p. 1.

[7] *AJP-3.10 – Allied Joint Doctrine for Information Operations*, November 2009, pp. 1-8.

Bibliografie:

1. *AJP-3.2 – Allied Joint Doctrine for Land Operations*, March 2016.
2. *AJP-3.4.9 – Allied Joint Doctrine for Civil-Military Cooperation*, Edition A, February 2013.
3. *AJP-3.10 – Allied Joint Doctrine for Information Operations*, November 2009.
4. *TRADOC Pamphlet 525-69 – Concept for Information Operations*, Department of the Army, August 1995.
5. *Joint Publication 3-13 – Information Operations*, February 2006.
6. Timothy L. Thomas, *Dialectical Versus Empirical Thinking: Ten Key Elements of the Russian Understanding of Information Operations*, Special Study No. 98-21, Foreign Military Studies Office, September 1998.
7. Vinod Anand, „Chinese Concepts and Capabilities of Information Warfare”, *Strategic Affairs*, Volume 30, Issue 4, Institute for Defense Studies and Analyses, October 2006.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 225/2019

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Site: https://cssas.unap.ro